

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)
)
Protecting the Privacy of Customers of Broadband) WC Docket No. 16-106
and other Telecommunications Services)
)
)
_____)

**COMMENTS BY CONSUMER FEDERATION OF CALIFORNIA (CFC)
RELATED TO THE NOTICE OF PROPOSED RULEMAKING (NPRM)**

Richard Holober,
Executive Director

Carl Block,
Legal Intern

1107 9th Street, Suite 625
Sacramento, CA 95814
(916) 498-9608



May 27, 2016

The Consumer Federation of California is pleased to submit our comments for consideration by the Federal Communications Commission in the above-referenced matter.

About the Consumer Federation of California.

The Consumer Federation of California (“CFC”) is a non-profit consumer advocacy organization. Originally founded in 1960 as the Association of California Consumers, the CFC has worked to improve state and federal consumer protection laws. Each year, CFC testifies before the California Legislature on dozens of bills that affect millions of our state’s consumers, including laws regulating food safety, predatory lending, health care and health insurance, telecommunications subscribers’ rights, construction defects, retail sales practices, consumer fraud, and access to civil justice, as well as other issue areas affecting consumer rights. CFC also participates in advocacy before the US Congress and federal regulatory bodies, and intervenes in proceedings of the California Public Utilities Commission (CPUC) and the California Department of Insurance (CDI) in support of consumer regulations, and participates in court actions involving consumer law.

For the past fifteen years, privacy has been a central focus of our work. CFC was a founding member of Californians for Privacy Now, a coalition that helped to win enactment of the nation’s strongest financial privacy law (*Senate Bill 1 - Speier; Chapter 791, Statutes of 2003*). CFC has testified in support of numerous pending pieces of legislation that would strengthen privacy rights and protections against identity theft. In 2011 CFC was instrumental in negotiating language that amended *California Civil Code Sections 1747.02 and 1747.08, Song Beverly Credit Card Act*, to allow a narrow credit card privacy exemption for collection of credit card holder zip codes for the limited purpose of preventing fraud or identity theft in card-not-present transactions at gas station fueling kiosks (*AB 1219 - Perea; Chapter 690, Statutes on 2011*). CFC sponsored a 2014 law (*AB 2667 – Bloom; Chapter 426, Statutes of 2014*) which stopped rent to own companies from secretly placing spyware on rental computers.

In 2013 CFC sponsored legislation (*SB 383 – Jackson*) which would have clarified the inclusive intent on the *Song Beverly Credit Card Act* following the State Supreme Court decision in *Apple Inc. vs. The Superior Court of Los Angeles County and David Krescent, S199384*, which ruled that credit card consumer privacy rights did not apply to online transactions involving downloadable products or services. In 2015 CFC sponsored *AB 886 (Chau)* which would have restricted the sharing of sensitive passenger information by app-based transportation network companies.

CFC led the legislative effort that stopped two attacks on *California’s Confidentiality of Medical Information Act, Civil Code Section 56 – 56.37*, by amending *AB 439 (Skinner)* in 2012 and *AB 1755 (Gomez)* in 2014, to eliminate language restricting patient access to the civil justice system in the event of a negligent release of individually identifiable medical information. CFC

helped craft smart grid consumer privacy requirements in a CPUC proceeding in *Rulemaking 08-12-009, Decision D. 14-05-016*. We petitioned the CPUC to initiate a mobile phone privacy rulemaking proceeding in *Petition P. 12-11-006*, (petition dismissed without prejudice) and testified in Department of Insurance regulatory proceedings restricting insurer access to a motorist's automobile's transponder data that is not germane to California automobile insurance rating factors (*Proposed Amendments to CCR 2642.4 et. Seq., Auto Rating Factors; Mileage Verification*).

A partial list of privacy laws that CFC helped enact include protecting the privacy of public school students' online activities (*SB 1177 – Steinberg, Chapter 839, Statutes of 2015*), extending library patrons' privacy rights to readers and purchasers of eBooks (*SB 602 – Yee, Chapter 424, Statutes of 2011*), limiting the use of data collected from transportation agencies' toll collecting transponders (*SB 1268 – Simitian, Chapter 489, Statutes of 2010*), requiring cell phones sold in our state to contain locking mechanisms to protect a consumer's privacy in case of a theft (*SB 962 – Leno, Chapter 275, Statutes of 2014*), strengthening the data breach notification law (*SB 24 – Simitian, Chapter 197, Statutes of 2011*), and extending medical privacy law to cover computer software and hardware, including app-based systems offered to consumers (*AB 658 – Ian Calderon, Chapter 296, Statutes of 2013*).

The FCC has the Authority to Protect Broadband Users.

The CFC applauds the FCC's move to improve consumer privacy. Consumers should control the collection, use and sharing of their private data. Securing this personal data requires transparency, fairness, consumer choice, and data security. To further this goal, the FCC should establish regulations which restrict broadband Internet access service (BIAS) providers from sharing personal consumer data for purposes that are not required to provide the access service for which the consumer enters into a relationship with the BIAS provider. The FCC should stop BIAS providers from charging for privacy. The FCC should set rules requiring any privacy choice notice to clearly state that opting-in to information sharing is not required to obtain service, and that opting-out from affiliate sharing does not affect the provision of Internet access service. The FCC should prohibit BIAS providers from compelling arbitration in disputes with consumers. The FCC should eliminate the 30-day waiting period for opting-out. The FCC should adopt the California Financial Code's definition of an "affiliate." And the FCC should broaden the definition of a consumer to protect the privacy of all people who share a broadband Internet connection.

The FCC has the authority to protect the privacy of broadband users. Congress granted the FCC the authority to regulate interstate communications by radio and wire in the *Communications Act of 1934, 47 U.S. Code § 151*. Broadband Internet Access Service is a

communications service provided by wire or radio to transmit data over the Internet; therefore, it fits within the areas that can be regulated by the FCC. 47 C.F.R. § 8.2. When a court reviews an agency's construction of the statute that it administers, if the statute is silent or ambiguous with respect to the specific issue, the question for the court is whether the agency's answer is based on a permissible construction of the statute. *Chevron, U.S.A., Inc. v. Nat. Resources Def. Council, Inc.*, 467 U.S. 837, 842-43 (1984). (The Supreme Court reversed a lower court ruling, finding that the Environmental Protection Agency's interpretation of the Clean Air Act was a permissible construction, and entitled to deference). Therefore, the FCC's interpretation of 47 U.S. Code § 151 is entitled to deference.

Both the FCC and FTC recognize that they have authority over different parts of the Internet. The FCC regulates BIAS providers, because Broadband Internet Access Service is provided by radio, wire, satellite or cable, in accordance with 47 U.S. Code § 151. The FTC has authority over Internet edge providers, under the FTC's dual mission of protecting consumers and promoting competition¹. To that end, the FCC and FTC signed a memorandum of understanding where each agency recognizes the others' expertise and agreed to coordinate and consult on areas of mutual interest².

We do not see a reason that the FCC and FTC need to implement regulations simultaneously. The FCC is implementing regulations within its sphere of responsibility. We look forward to the FTC coordinating, and enacting similar regulations within its sphere of responsibility. It would needlessly delay protections for consumers if the government requires that the FCC and FTC implement their regulations simultaneously.

The FCC Should Protect Consumer Privacy Because of the Unique Role of Broadband Internet Access Service Providers.

At the core of the FCC proceeding is the question of whether BIAS providers should be entitled to collect from a consumer personal data that are not germane to the completion of transactions for which the consumer enters into the relationship with the Internet provider, and use or share that data with third parties for purposes of private gain, or other purposes that are

¹ *What We Do*, FTC, <https://www.ftc.gov/about-ftc/what-we-do>, accessed 17 May 2016. *Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information*, FTC, <https://www.ftc.gov/news-events/press-releases/1998/08/Internet-site-agrees-settle-ftc-charges-deceptively-collecting>, accessed 17 May 2016.

² *Memorandum of Understanding on Consumer Protection Between the FTC and the FCC*, November 16, 2015, available at <https://www.ftc.gov/policy/cooperation-agreements/memorandum-understanding-consumer-protection-between-federal-trade>, accessed 15 May 2016.

not related to providing the service to the consumer. We believe that personal privacy is a fundamental right of American residents and consumers, and that utilization of a product or service should not require a consumer to waive that right for any purpose that is not required to provide that service or product, or to comply with a law.

A consumer expects to pay a fair price to receive a properly functioning product or a reliable service. When engaging in a transaction, a consumer may be required to provide personal information. It may be the consumer's name when paying for a meal using a credit card, name and address when registering a new toaster for warranty purposes, or credit history when applying for a mortgage. The consumer expectation is that the information is provided to complete the transaction, and not for other purposes. A business should not conceal, or obfuscate in legalistic fine print that a consumer is not likely to read or understand, that the business uses or shares consumer information for purposes that are not germane to the use of the service or product.

Consumers care about protecting their personal privacy. Protecting consumer identification information such as name address, phone number, credit card number, social security number and email address are of vital importance in all business transactions. Online technologies, including the Internet, pose new and heightened privacy concerns that may not be prevalent in "brick and mortar" transactions, because these technologies allow businesses to snoop with ease into one's personal life in ways that could not have been contemplated twenty years ago. Research shows the heightened concern Americans have about loss of their personal privacy when they are online³.

BIAS providers have a unique and distinct role to access the network services. The FCC should ensure privacy protections for consumers of broadband because consumers must use a BIAS provider to access Internet services, and consumers cannot easily substitute a BIAS provider. Additionally, BIAS providers see all Internet traffic that comes from a consumer.

Consumers must use BIAS providers to access the Internet. Network protocols are conceptually designed using the seven layer Open Systems Interconnection (OSI) model, as defined in International Standards Organization (ISO) Reference Standard 7498⁴. BIAS providers deliver services at the four lowest layers of the model: the physical layer, the data link

³ Marry Madden and Lee Rainie, *Americans' Attitudes about Privacy, Security and Surveillance*, Pew Research Center, May 20, 2015, available at <http://www.pewInternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>, accessed May 22, 2016.

⁴ International Standards Organization Reference Standard 7498, *Open Systems Interconnection – Basic Reference Model*, 1996, accessed May 22, 2016.

layer, the packet networking layer, and the transport layer.⁵ Internet edge providers, such as Google or CNN, do not provide services at the lowest layers of the model. Internet edge providers provide services at the highest three layers of the model: the application layer, presentation layer, and session layer.

Consumers must use the physical layer, data link layer, packet networking layer and transport layer of a network in order to get to any edge provider. Broadband services provide the physical layer, usually in the form of a cable, or Digital Subscriber Line (DSL), or radio frequency connection. Broadband providers use the data link layer to transmit bits in the form of a frame between two nodes in a network. Broadband providers route packets of frames to different servers using the packet networking layer. Broadband providers use the transport layer to deliver reliable transmission of data between points in the network, via acknowledgement of packets and forward error correcting protocols. Consumers cannot get to the services of an edge provider without using the lower layers of the OSI model delivered by a BIAS provider.

Consumers cannot easily substitute a BIAS provider. BIAS providers are usually physically connected by wires or cables to the consumer's residence. If a consumer wants to switch a physically connected BIAS provider, the consumer must call the old provider to terminate the Internet service and disconnect, and call the new provider to establish a new customer relationship, after which the new BIAS provider will set a service date to connect new wires. In some cases, BIAS providers are connected via radio transmissions. If a consumer receives Internet via radio transmission, to switch BIAS providers, the consumer must terminate the customer relationship and disconnect the radio transceiver from the old service, and have the new BIAS provider send and connect a new transceiver after first establishing a contractual relationship as a new customer. Regardless of the nature of the connection, it may require the consumer to agree to a credit check by the new BIAS provider. In some cases, a BIAS provider may establish a minimum contractual service period of one year or more, with financial inducements for agreeing to the minimum contract period or penalties for early termination of a service contract.

Even if a consumer could easily substitute a BIAS provider, consumers are usually limited to the local dominant telephone provider and the local dominant cable television provider. Consumers do not have a wide variety of choices in BIAS providers. They can only use the services of BIAS providers who have invested in the infrastructure to deliver high-speed Internet in their local area.

BIAS providers are physically and logically different than edge providers. Unlike edge providers, BIAS providers cannot be easily substituted. Unlike edge providers, consumers

⁵ *OSI Model*, Wikipedia, accessed May 22, 2016.

usually do not have a wide choice of BIAS providers. The effort required to substitute a BIAS provider is much greater than the effort required to change an edge provider. If a consumer wants to switch to a different news service on the Internet, they just type the name of the different news service into a search engine and start using that address. The consumer is free to switch search engines, again by typing in the name of a different search engine and linking to that search engine. No physical changes are needed. No contractual relationship is established. With rare exceptions, no payment is required to initiate service. The switch is virtually instantaneous, free, and requires no commitment of continuity by the consumer. In stating this we are not suggesting that edge providers should have any greater latitude to collect or share personal information. On the contrary, unfair and abusive intrusion into Internet users' personal information is a universal problem. But given the position of BIAS providers as the gateway to the Internet, and given the FCC's jurisdiction over BIAS providers, we believe it is essential to establish privacy protections as envisioned in this proceeding.

BIAS providers are capable of tracking, collecting and storing a consumer's online browsing and search activities, and combining that information with the consumer's name, address, email address, phone number, bank account or credit card information, and other personal information that the BIAS provider collects in the course of its business transactions with the consumer. This information can reveal a wealth of individually identifiable information about a consumer.

To mention a few types of data that the BIAS provider is positioned to collect and aggregate with a consumer's name and other personal information: searches about a disease and/or visits to websites that describe a disease may provide information about a consumer's mental or physical health condition (e.g. searches on the topic of alcoholism and visits to alcoholism treatment websites could lead to characterization of the consumer as an individual suffering from the disease or living in a household with an alcoholic); searches of and/or visits to political causes or candidates may reveal a consumer's political views; searches of and/or visits to online dating sites may reveal information about the consumer's love life; searches of and/or visits to LGBT-focused information may identify a consumer's sexual orientation; searches of and/or visits to banking and financial sites may reveal a consumer's financial status (e.g. Internet activity related to payday loans in the case of one low income consumer, or to brokerages and investment opportunities in the case of another, high wealth consumer); and other searches of and/or visits to sites that relate to hobbies, shopping interests, entertainment, leisure time activities or other personal or professional interests provide a treasure trove of information about a consumer that, combined with other data, creates an extensive profile that a BIAS provider can exploit for gain without the consumer's knowledge or consent.

BIAS providers should not share with third parties any of this data, with very limited exceptions that we outline below.

The FCC should Stop Businesses from Charging for Internet Privacy.

The NPRM requests comment on financial inducement practices. *NPRM Para. 259*. The Consumer Federation of California recommends the FCC not allow financial inducements for privacy. AT&T is deploying a new “GigaPower” BIAS service in markets throughout the country. It has offered customers of this service a discount of roughly \$30 per month if they allow AT&T to track and use their individual web browsing information in order to tailor ads and offers to the customers’ interests. Other businesses are eager to roll-out similar programs⁶. AT&T has stated that, since it debuted the program, the majority of customers offered the option have elected to accept the discount in return for reduced privacy⁷.

Another way to think of the AT&T offer is that consumers who want privacy have to pay \$30 extra per month, or \$360 per year, as opposed to those who do not get privacy. AT&T is not offering this program because it is benevolent. Consumer behavior information is extremely valuable. AT&T will make money by selling consumers’ information, or access to that information, to third parties, if they accept the financial inducement. AT&T also makes money by charging the consumer what is in effect a premium surcharge for privacy, if the consumer is unwilling to allow AT&T to snoop into their private information that is transmitted over the network. Either way, AT&T wins, and the consumer loses.

A fundamental problem with charging \$360 per year for not monitoring, recording and sharing consumer web traffic is that only the wealthiest consumers will be able to afford privacy. Low and moderate income consumers will never be able to afford privacy.

The “digital divide” is an economic and social inequality with regard to access to the Internet⁸. The “digital divide” was first identified over a decade ago, and continues today⁹. The Pew Research Center identified that cost continues to be a significant factor in Americans that do

⁶ Stacey Higginbotham, *ISPs really, really want to be able to share your data*, Forbes, (Apr 28, 2015), available at <http://fortune.com/2015/04/28/isps-share-your-data/>, accessed 15 May 2016.

⁷ Natsha Singer, *AT&T’s Offer: Share Your Data for Personalized Ads, or Pay More*, N.Y. Times (Feb 18, 2015), available at http://bits.blogs.nytimes.com/2015/02/18/atts-offer-share-your-data-for-personalized-ads-or-pay-more/?_r=0, accessed 15 May 2016.

⁸ *Digital Divide*, Wikipedia, available at https://en.wikipedia.org/wiki/Digital_divide, accessed 22 May 2016.

⁹ Council of Economic Advisors Issue Brief, *Mapping the Digital Divide*, July 2015, available at https://www.whitehouse.gov/sites/default/files/wh_digital_divide_issue_brief.pdf, accessed on 22 May 2016.

not have access to the Internet¹⁰. By taking advantage of consumers, BIAS providers are increasing the digital divide in the area of privacy. Only the wealthiest and most astute consumers will choose to afford privacy.

This monetary penalty for privacy impacts the poor the greatest. But it also impacts hundreds of millions of moderate income Americans. 62% of American workers live paycheck to paycheck.¹¹ As many as 36% of workers have less than \$1000 saved for retirement.¹² Research shows that Americans hold strong views about protecting online privacy¹³. Unfortunately, the financial straits that Americans find themselves in will inexorably lead most to waive their privacy as the price they must pay to survive in a world where Internet access has become a basic necessity of life.

In addition to affordability, consumers have difficulty placing a monetary value on privacy. Consumers have little knowledge of the details or extent of the personally identifiable data that is collected or shared by their BIAS providers and others. BIAS providers are taking advantage of the consumer's lack of understanding of the value of privacy and of the content of the personal information that is collected. Understanding the monetary value of privacy is important, but it is only one dimension of the value that Americans place in our privacy. Of equal or greater importance is our distaste for unwarranted intrusion into our lives, whether it be the compiling of sensitive information regarding a person's health status, sexual orientation or political views, or our discontent with any unwelcome snooping into and sharing of our shopping habits, entertainment viewing, or individual human curiosity as demonstrated by our online activities. A BIAS provider may consider the collection and sharing of this information innocuous, but consumers disagree.

¹⁰ Pew Research Center, *Digital Divides 2015*, September 22, 2015, <http://www.pewInternet.org/2015/09/22/digital-divides-2015/>, accessed on 22 May 2016.

¹¹ Quentin Fottrell, *Most Americas are One Paycheck Away from the Street*, MarketWatch, January 31, 2015, available at <https://secure.marketwatch.com/story/most-americans-are-one-paycheck-away-from-the-street-2015-01-07>, accessed on May 26, 2016

¹² Nanci Hellmich, *Retirement, a third have less than \$1000 put away*, USA Today, April 1, 2014 available at <http://www.usatoday.com/story/money/personalfinance/2014/03/18/retirement-confidence-survey-savings/6432241/>, accessed May 26, 2016

¹³ Marry Madden and Lee Rainie, *Americans' Attitudes about Privacy, Security and Surveillance*, Pew Research Center, May 20, 2015, available at <http://www.pewInternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>, accessed May 22, 2016.

The FCC Should Eliminate the 30-Day Waiting Period for Opting-Out.

The NPRM requests comment on the framework to give broadband customers tools to make informed and timely decisions about how BIAS providers can use their information. *NPRM Para. 27.* The FCC proposes that BIAS providers must provide a customer with notice and the opportunity to opt-out before they may use that customer's Privacy Information, or share such information with an affiliate that provides communications-related service, to market communications related services to that customer. *NPRM Para. 122.* We agree. BIAS providers should not be allowed to discourage a consumer from opting-out from affiliate information sharing. The opt-out notice should be presented in a manner that is prominent, easy to access, easy to read, written in non-legalistic jargon, and that is available at the time the consumer signs up for or activates the service, and at all other times when accessing the Internet.

The Consumer Federation of California concurs with the FCC proposal to eliminate the 30-day waiting period currently required to make a voice-customer's opt-out approval effective. *NPRM Para. 68.* The older 30-day rule was based on a manual process where employees needed to route paperwork throughout an organization to implement an opt-out request. Computers route traffic and collect information from across the Internet. Computers do not take 30-days to stop collecting information on a consumer. Computers do not take 30-days to stop transmitting information to an affiliate. Consumers expect a faster response. We applaud the FCC's proposal to eliminate the 30-day waiting period.

The FCC Should Clarify that Opting-In Is Not Required to Obtain Service.

BIAS providers should not be permitted to encourage opting-in to information sharing with other non-affiliated third parties. CFC recommends that the FCC specifically state that an opt-in notice should be presented to the consumer in such a manner that it is not perceived by the consumer as part of the service. The decision to opt-in should be presented to the consumer at a separate time from initially signing-up for or activating the service, so the consumer does not perceive that opting-in is a condition of receiving the service. Any opt-in selection should be revocable at any time by the consumer. That revocation right should be easy to read and understand, and prominently featured in any opt-in consent form. It should also be prominently featured and easy to access and use on the BIAS provider's website.

The decision to opt-in or opt-out is only as good as it is understandable and easy to use. The Internet is filled with "click-wrap" agreements that consumers never read¹⁴. One website

¹⁴ Seth Stevenson, *By Clicking on This Article, You Agree To . . .*, Slate, Nov 17, 2014, available at

even embedded a \$1000 reward in their end user license agreement for anyone who read the agreement. Five months passed until someone claimed the reward¹⁵. The consumer needs easy to understand notices from the BIAS provider about the opt-in or opt-out choices. The *California Financial Information Privacy Act* is an excellent example of how decisions about privacy information should be communicated to the consumer. *Cal. Fin. Code § 4053(d)*. The law provides a form that a financial institution may use to comply with the required opt-out notice. The notice's opt-out language is simple, using clear and concise sentences. The opt-out form is a separate document. The consumer makes the choices by simply checking a box, adding name and account number, and returning it in the mail. In addition to a mandatory written form, the law allows the financial institution to facilitate a consumer's opt-out selection by providing a toll free phone number to call and/or website URL to visit to notify the company of an opt-out decision. An example of this simple language under the *California Financial Information Privacy Act* is in the appendix to this filing. In the twelve years since this law took effect, the financial services industry has not approached the legislature to modify it in any way.¹⁶

The FCC Should Prohibit BIAS Providers from Compelling Arbitration in their Contracts.

The NPRM requests comment on whether the FCC should prohibit BIAS Providers from compelling arbitration in their contracts. *NPRM Para. 274*. In the 2015 Open Internet Order, the FCC agreed that mandatory arbitration may frequently benefit the party with more resources and more understanding of the dispute procedure, and therefore should not be adopted¹⁷. In 2015, the Consumer Financial Protection Bureau issued an empirical arbitration study, which identified

http://www.slate.com/articles/technology/technology/2014/11/end_user_license_agreements_does_it_matter_that_we_dont_read_the_fine_print.html, accessed May 22, 2016.

¹⁵ *It Pays to Read License Agreements (7 Months Later)*, Tech Talk, June 12, 2012, available at <http://techtalk.pcpitstop.com/2012/06/12/it-pays-to-read-license-agreements-7-years-later/>, accessed May 22, 2016.

¹⁶ The 9th Circuit upheld *California Financial Information Privacy Act* in almost all regards (overturning only a state opt-out for information sharing with credit reporting agencies), *Am. Bankers Ass'n v. Lockyer*, 541 F.3d 1214, (9th Cir. 2008), *cert. denied sub nom. Am. Bankers Ass'n v. Brown*, 557 U.S. 935 (2009)

¹⁷ *2015 Open Internet Order*, FCC, Para. 267, available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf, accessed May 24, 2016.

that most consumers do not understand pre-dispute arbitration agreements¹⁸. The study surveyed 1,007 consumers and showed that 54.4% of those who had arbitration agreements in their credit card contracts did not know if they could sue the card issuer in court¹⁹. Over one third (38.6%) of consumers incorrectly believed they could sue in court²⁰. Only one out of 1,007 consumers recalled being offered an opt-out opportunity²¹.

The FCC should prohibit BIAS providers from compelling arbitration in their contracts. The Consumer Financial Protection Bureau report to Congress shows that consumers do not understand mandatory arbitration. Consumers should have the opportunity to voluntarily opt-in to arbitrate a dispute, provided the explanation of the arbitration option is in simple, brief, easy to understand language, and it clearly and prominently states that the consumer has an absolute right to adjudicate the dispute in a court of law, and further provided the voluntary opt-in is presented to the consumer after the consumer informs the BIAS provider that a dispute exists, not beforehand. The FCC should not allow an opt-out regime, because the Consumer Financial Protection Bureau report shows that the vast majority of consumers do not remember being offered an opt-out opportunity. If consumers do not remember receiving an opt-out opportunity, then opting-out of arbitration is an illusory choice.

The FCC Should Adopt the California Financial Information Privacy Act's Definition of an "Affiliate."

The NPRM seeks comment on how the FCC should define "affiliate" for purposes of the proposed rule. *NPRM Para. 30*. Current FCC rules define affiliate to mean "a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person," where the term "own" is defined to mean "to own an equity interest (or the equivalent thereof) of more than 10 percent."

The Consumer Federation of California recommends the FCC adopt the more stringent standards outlined in the *California Financial Information Privacy Act*. Under this California

¹⁸ Consumer Financial Protection Bureau, *Arbitration Study, Report to Congress, pursuant to Dodd-Frank Wall Street Reform and Consumer Protection Act, § 1028(a)*, March 2015, http://files.consumerfinance.gov/f/201503_cfpb_arbitration-study-report-to-congress-2015.pdf, accessed May 24, 2016.

¹⁹ *Id.* at Section 3.1, pg. 3.

²⁰ *Id.* at Section 3.1. pg. 3.

²¹ *Id.* at Section 3.1, pg. 4.

privacy law, “control” means (1) ownership or power to vote 25 percent or more of the outstanding shares of any class of voting security of a company, acting through one or more persons, (2) control in any manner over the election of a majority of the directors, or of individuals exercising similar functions, or (3) the power to exercise, directly or indirectly, a controlling influence over the management or policies of a company. *Cal. Fin. Code § 5042(g)*.

The purpose of the more stringent “25 percent” ownership or control of the election of a majority of directors is to narrow the number of business relationships that can be considered affiliates. The plain English definition of the noun affiliate states “an organization (such as a television station) that is a member of a larger organization (such as a national network).”²² This definition describes an intimate relationship of common ownership and control, such as a corporate parent to its subsidiary, or sister corporate entities under the control of the same corporate parent. Plain English, as consumers commonly understand the word, does not view an affiliate relationship to consist of 10% or even 25% ownership. Instead, it connotes majority ownership and control.

Adopting the above-referenced California definition of affiliate would bring the FCC’s definition closer to the commonly used and commonly understood plain English dictionary definition. Narrowing the number of relationships that are considered affiliates would have the practical effect of limiting the “junk mail” that floods the email boxes of consumers. If a consumer wants to receive additional email from vendors who do not meet the 25 percent standard, the consumer can always choose to “opt-in.” It also narrows the amount of targeted online advertisements, many of which are camouflaged as valid information search results that mislead, annoy and intrude into the private personal space that consumers seek when searching the web.

Some may argue that this will “shackle” BIAS providers. We disagree. Research from the Massachusetts Institute of Technology shows that when consumers are offered a choice, they choose a vendor who provides greater privacy²³. Pew Research shows that Americans hold a strong view about “being in control of who can get information about you.”²⁴ The combination

²² <http://www.merriam-webster.com/dictionary/affiliate>, accessed May 27, 2016.

²³ Nic Fleming, *Just How Much is Your Privacy Worth?*, MIT Technology Review, March 21, 2012, available at <https://www.technologyreview.com/s/427289/just-how-much-is-your-privacy-worth/>, accessed May 22, 2016.

²⁴ Marry Madden and Lee Rainie, *Americans’ Attitudes about Privacy, Security and Surveillance*, Pew Research Center, May 20, 2015, available at <http://www.pewInternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>, accessed May 22, 2016.

of the MIT research and Pew research indicates that BIAS providers who allow consumers to control who can get information about their Internet usage will be preferred by consumers.

The FCC Should Broaden the Definition of a Customer.

The FCC requests comment on whether the definition of a “customer” should reflect the possibility of multiple broadband users. *NPRM Para 34 – 36.*

Consumer Federation of California concurs with the FCC proposal that the current definition of a customer is far too narrow. The current narrow definition of a customer is “a person or entity to which the telecommunications carrier is currently providing a service.” *47 C.F.R. § 64.2003(f)*. We recommend a broad definition of the customer, which is in keeping with what a reasonable consumer of network services would understand. The definition of customer should not merely include that single person who is in privity with the BIAS. It is very common for families to share a single Internet connection. It is common for people to allow their guests to use their Internet connection. If a consumer chooses to not allow BIAS providers to track their network traffic, then the reasonable consumer will also assume that choice applies to all other people using the same Internet connection.

Under the 2015 Network Neutrality Rules, the FCC identifies an end user as “any individual or entity that uses a broadband Internet access service.” *47 C.F.R. § 8.2*. We recommend harmonizing the definition of “customer” with “end user.” Harmonizing “customer” with the current definition of “end user” meets the expectations of a reasonable Internet consumer.

Conclusion.

The Consumer Federation of California applauds the FCC’s step forward to improve consumer online privacy. To further this goal, the FCC should stop companies from charging for privacy. The FCC should adopt the California definition of an “affiliate.” Additionally the FCC should ensure consumers understand that Opting-In is described in easy to understand language that makes it clear that it is not required to obtain or utilize Internet service. Further, the FCC should eliminate the 30-day waiting period for opting-out. It should be offered as soon as a consumer signs up for or activates a BIAS service. And the FCC should broaden the definition of a consumer to protect the privacy of all people who share a broadband Internet connection.

We thank the Federal Communications Commission for considering our comments.

Appendix

Cal. Fin. Code § 4053(d)

Important Privacy Choices for Consumers

You have the right to control whether we share some of your personal information. Please read the following information carefully before you make your choices below.

Your Rights

You have the following rights to restrict the sharing of personal and financial information with our affiliates (companies we own or control) and outside companies that we do business with. Nothing in this form prohibits the sharing of information necessary for us to follow the law, as permitted by law, or to give you the best service on your accounts with us. This includes sending you information about some other products or services.

Your Choices

Restrict Information Sharing With Companies We Own or Control (Affiliates): Unless you say “No.” we may share personal and financial information about you with our affiliated companies.

NO, please do not share personal and financial information with your affiliated companies.

Restrict Information Sharing With Other Companies We Do Business With To Provide Financial Products And Services: Unless you say “No,” we may share personal and financial information about you with outside companies we contract with to provide financial products and services to you.

NO, please do not share personal and financial information with outside companies you contract with to provide financial products and services.

Time Sensitive Reply

You may make your privacy choices(s) at any time. Your choice(s) marked here will remain unless you state otherwise. However, if we do not hear from you we may share some of your information with affiliated companies and other companies with whom we have contracts to provide products and services.

Name: _____

Account or Policy Number(s): _____ [to be filled in by consumer]

Signature: _____

To exercise your choices do [one of] the following:

(1) Fill out, sign and send back this form to us using the envelope provided (you may want to make a copy for your records); [#1 is mandatory]

[(2) Call this toll-free number (800) xxx-xxxx or (xxx) xxx-xxxx]; [optional]

[(3) Reply electronically by contacting us through the following Internet option: xxxxx.com) [optional]